Karthik S Arkasali

919606746816 karthik.arkasali@gmail.com LinkedIn Portfolio

PROFESSIONAL SUMMARY

Proactive entry-level cybersecurity professional with hands-on experience in SIEM, SOAR, EDR, and threat intelligence. Skilled in analyzing and responding to security threats using tools like Splunk and Wazuh to enhance detection and response. Passionate about safeguarding assets and contributing to resilient cybersecurity strategies.

EDUCATION

Bachelor of Engineering in Electronics & Communication July 2022

Sapthagiri College Of Engineering | Bangalore, India

TOOLS & TECHNOLOGIES

- **Security Tools**: Splunk, Wazuh, Kibana
- **SOAR Platforms:** Tines, Shuffle
- **Threat Detection:** LimaCharlie, Elastic Defend, Honeypot
- **Vulnerability Scanning:** Nessus, OpenVAS
- **Malware Analysis:** FlareVM, Mimikatz, LaZagne
- **Programming & Scripting:** Python, SQL
- **Frameworks & Methodologies:** Cyber Kill Chain, NIST (CSF), ISO 27001, PCI DSS

TECHNICAL SKILLS

- Hands-on experience with **Security Information & Event Management** tools, including Splunk, Wazuh, and Kibana.
- Proficient with **Network Security** devices such as Firewalls, Virtual Private Network, Proxies, and IPS/IDS systems.
- Knowledgeable in malware analysis and the **OWASP Top 10** vulnerabilities.
- Expertise in **Analysing Incidents** using the Cyber Kill Chain framework and MITRE ATT&CK methodology.
- Skilled in developing **Automated workflows** to streamline incident response and reduce downtime.

PROJECTS

Automated Threat Response and Detection with Endpoint Detection & Response | Project Link

- **Achievement**: Enhanced detection accuracy by 25% and reduced incident response time by 30% through automation.
- **Method**: Configured LimaCharlie for real-time threat telemetry and developed Slack/email notification workflows for rapid response.

Proactive Threat Detection with Elasticsearch, Logstash, & Kibana (ELK) Stack | Project Link

- **Achievement:** Reduced containment times by 40% and alert analysis time by 20% through real-time dashboards.
- **Method:** Configured Elasticsearch, Logstash, and Kibana (ELK) to monitor SSH/RDP logs and integrated Elastic Defend for automated system isolation upon detection.

CERTIFICATION

- **Google Cybersecurity Certificate -** Developed expertise in SIEM and incident response, enhancing foundational and advanced security skills. **Certificate Link**
- **Cybersecurity Virtual Experience Program on Forage -** Hands-on exposure to phishing simulations, incident analysis, and awareness program design. **Certificate Link**